AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the subject application:

Listing of Claims:

1. – 17. (Cancelled)

18. (Previously Presented) A method, comprising:

reading a media key block from a medium, the medium having content and validation data that includes a validation value;

generating a media key from the media key block;

reading the validation data;

decrypting the validation data using the media key; and

granting access to the content if the validation data decrypts to the validation value.

19. (Previously Presented) The method of claim 18, wherein said reading the validation data comprises reading a copy of the validation data from a read-only area of the medium.

20. (Previously Presented) The method of claim 18, wherein said reading the validation data comprises reading the validation data from a read only area of the medium.

21. (Previously Presented) The method of claim 20, wherein the validation data comprises a hash value based on the media key block.

22. (Previously Presented) The method of claim 21, wherein the hash value is stored in a validation area of the medium.

23. (Previously Presented) The method of claim 18, wherein the validation data comprises a verification data field of a verify media key record of the media key block.

24. (Currently Amended) A system comprising:

a drive to:

read a hash value from a validation area of a medium having content, ~~the medium having content, and a media key block~~; and

read a media key block from the medium; and

a host to:

~~read the media key block from the medium; and~~

calculate a hash function over the media key block.

25. (Previously Presented) The system of claim 24, additionally comprising:

the drive to further:

calculate a MAC (message authentication code) over the hash value to generate a drive MAC value; and

generate a second hash value based on the media key block; and

the host to further:

calculate the MAC over the second hash value to generate a host MAC value;

compare the drive MAC value to the host MAC value; and

grant access to the content if the drive MAC value equals the host MAC value.

26. (Previously Presented) The system of claim 24, wherein the medium comprises a DVD-RAM (Digital Versatile Disc – Random Access Memory), and the hash value is stored in a control data area of the DVD-RAM.

27. (Previously Presented) An apparatus comprising:

a device to:

read a medium having content, a media key block, and a copy of the verification data corresponding to a verification data field of the media key block, the verification data field being associated with a predetermined value;

process the media key block to generate a media key;

decrypt the copy of the verification data using the media key; and

grant access to the content if the copy of the verification data decrypts to the predetermined value.

28. (Previously Presented) The apparatus of claim 27, wherein the medium comprises a DVD-R/W (Digital Versatile Disc –Rewriteable), and the copy of the verification data is stored in a narrow burst cutting area of the DVD-R/W.

29. (Previously Presented) The apparatus of claim 28, wherein the medium additionally comprises a hash value based on the media key block, the hash value being stored in the narrow burst cutting area of the DVD-R/W.